

# The information cost of quantum memoryless protocols

André Chailloux\*, Iordanis Kerenidis†, Mathieu Laurière‡

March 10, 2017

## Abstract

We consider memoryless quantum communication protocols, where the two parties do not possess any memory besides their classical input and they take turns performing unitary operations on a pure quantum state that they exchange between them. Most known quantum protocols are of this type and recently a deep connection between memoryless protocols and Bell inequality violations has been explored in [11]. We study the information cost of memoryless quantum protocols by looking at a canonical problem: bounded-round quantum communication protocols for the one-bit AND function. We prove directly a tight lower bound of  $\Theta(\frac{\log k}{k})$  for the information cost of AND for  $k$ -round memoryless quantum protocols and for the input distribution needed for the Disjointness function.

It is not clear if memoryless protocols allow for a reduction between the AND function and Disjointness, due to the absence of private workspaces. We enhance the model by allowing the players to keep in their private classical workspace apart from their classical input *also* some classical private coins. Surprisingly, we show that every quantum protocol can be transformed into an equivalent quantum protocol with private coins that is perfectly private, i.e. the players only learn the value of the function and nothing more. Last, we consider the model where the players are allowed to use one-shot coins, i.e. private coins that can be used only once during the protocol. While in the classical case, private coins and one-shot coins are equivalent, in the quantum case, we prove that they are not. More precisely, we show that every quantum memoryless protocol with one-bit inputs that uses one-shot coins can be transformed into a memoryless quantum protocol without private coins and without increasing too much its information cost. Hence, while private coins always allow for private quantum protocols, one-shot coins do not.

## 1 Introduction

### 1.1 Context

In the model of communication complexity, two players, Alice and Bob, receive inputs and would like to solve some distributed task that depends on these inputs, while minimizing the number of bits they exchange. This model has deep connections to many areas of computer science, including data structures, circuit lower bounds and streaming algorithms [22].

Recently, a lot of attention has been given to a different measure of complexity for communication protocols, namely the amount of information that is leaked about the players inputs during the protocol. The information cost of a protocol is always lower than the communication cost, since one communicated bit can carry at most one bit of information. It has proved to be one of the strongest techniques we have to lower bound the communication complexity of functions [3, 7, 4, 19].

One can also define the notions of communication and information complexity in the quantum setting, where the two players exchange quantum messages. While it is straightforward to define the communication cost of a quantum protocol as the number of qubits that the two players exchange, one has to be careful when defining the information cost of a quantum protocol.

Besides some application-specific definitions [18, 17], recently two main definitions have been put forward. Touchette [27] has defined a notion of quantum information cost (QIC) and has proved that it has a number of important properties, including that for any function the quantum information complexity, namely the information cost of the optimal quantum protocol that solves the function, equals the amortized communication complexity of the function. Kerenidis et al. [20] proposed a different notion, the classical input information

---

\*Inria, Paris, [andre.chailloux@inria.fr](mailto:andre.chailloux@inria.fr)

†CNRS IRIF, Université Paris 7, [jkeren@liafa.univ-paris-diderot.fr](mailto:jkeren@liafa.univ-paris-diderot.fr)

‡NYU-ECNU Institute of Mathematical Sciences at NYU Shanghai, [mathieu.lauriere@nyu.edu](mailto:mathieu.lauriere@nyu.edu)

cost (CIC), that is more intuitively related to the information leakage of the protocol, but is smaller than the QIC notion. Very recently, Laurière and Touchette [24] clarified the relation between the two notions showing that while CIC measures how much information each player learns about the other’s input during the protocol, the QIC measures, on top of this, the information the players forget during the protocol.

While our understanding of the flow of information during a quantum protocol has deepened, both these notions remain difficult to use in practice. The main reason is that mathematically they both involve a quantum conditional mutual information, where the conditioning is on a quantum variable. This quantity is notoriously difficult to handle, even though there has been some recent breakthrough work on it [13].

Here, we try to overcome this difficulty by looking at a rich subclass of quantum protocols that we call *memoryless* quantum protocols. In these protocols, the two parties take turns performing unitary operations on a pure quantum state that they exchange between them. In other words they do not possess any memory and hence they do not keep anything in their private space apart from their classical input.

There are many reasons why it is interesting to look at such protocols. First, almost all quantum protocols we know are memoryless. This includes all protocols in the simultaneous message passing model, eg. fingerprints for Equality [9], and in the one-way model, e.g. Hidden Matching [2, 15], but also the two-way protocol for Disjointness in [10] and for Vector in Subspace [26, 21]. We note that the optimal protocol for Disjointness by Aaronson-Ambainis [1] is not described as a memoryless protocol. Second, there is a deep connection between memoryless protocols and Bell inequality violations that has been explored in [11, 23]. Third, moving towards implementations of quantum communication protocols and the realization of quantum networks, memoryless protocols can be much easier to implement as it has already been shown [28, 16]. Last but not least, we will argue it may be easier to understand the flow of quantum information in memoryless protocols. For example, it is easy to see that the relation between the two notions, CIC and QIC, is in this case clear: for any memoryless protocol, QIC is exactly two times the CIC, since the players forget exactly as much as they learn. Note that forgetting is not necessarily a drawback of quantum protocols: forgetting can be required in order to obtain quantum communication speed-ups, as shown in [24].

## 1.2 Contributions

In our work, we study the information cost of memoryless quantum protocols by looking at a canonical problem: bounded-round quantum communication for the AND function, where the players receive one bit each and their goal is compute the AND of the inputs.

One of the main reasons to study the AND function is its close relation to the Disjointness problem (DISJ), where the players receive one set each and their goal is to decide whether these two sets are disjoint. One can see DISJ as a function that takes as inputs two  $n$ -bit strings  $x, y$  and returns the OR of the coordinate-wise AND of these strings, i.e.  $\text{DISJ}(x, y) = \text{OR}(\text{AND}(x_1, y_1), \dots, \text{AND}(x_n, y_n))$ . In the classical world, a very elegant lower bound for Disjointness using information-theoretic tools was given by Bar-Yossef et al. [3] and its proof consists of the following two steps: first, one can reduce DISJ to AND. Namely, given a protocol for DISJ on inputs of size  $n$ , the players can construct a protocol to solve AND in the following way: they embed their one-bit inputs for AND in some random coordinate for DISJ, use their private coins to pick the remaining  $(n - 1)$  inputs uniformly from  $\{(0, 0), (0, 1), (1, 0)\}$ , and run the DISJ protocol. The output of DISJ for such inputs is the same as the output of the AND function. One can show this way that if the information cost of the DISJ protocol is  $I$ , then the information cost of the new protocol for AND is  $I/n$ . This implies the information complexity of DISJ is at least  $n$  times the information complexity of AND for the above input distribution. The second stage, involves computing directly the information complexity of the AND function, and showing to be at least a constant, the tight  $\Omega(n)$  lower bound for DISJ is obtained. This result not only gives a simpler proof of the DISJ lower bound but it has sparked the interest for the study of information complexity that has led to numerous advances [7, 4, 6, 8].

In the quantum world, things are considerably more complicated. The first attempt to provide an information-theoretic proof of the bounded-round quantum communication complexity of DISJ was by Jain et al. [18]. In their work, they used a different information-theoretic notion from QIC and CIC and used it to reduce the DISJ problem to the AND problem. By directly lower bounding this quantity for the AND function they managed to get a lower bound of  $\Omega(n/k^2)$ , for any  $k$ -round protocol for DISJ. There is no clear way to improve this lower bound using their information-theoretic notion and this bound falls short of the optimal bound of  $\Omega(n/k)$ . Very recently, [5] provided a proof which gives an almost optimal bound of  $\tilde{\Omega}(n/k)$  for  $k$ -round protocols for DISJ by reducing DISJ to AND and then using the already known lower bound for DISJ to lower bound the complexity of AND. Note that this proof does not provide a direct proof for the information complexity of AND.

In our work we prove directly a tight lower bound for the information complexity of AND for memoryless

protocols and for the input distribution needed for DISJ. More precisely, considering the input distribution  $\mathcal{U}_0$  defined by  $\mathcal{U}_0(x, y) = \frac{1}{3}$  for  $(x, y) \neq (1, 1)$  and  $\mathcal{U}_0(1, 1) = 0$ , we show the following, where  $\text{CIC}_{\mathcal{U}_0, \varepsilon, k}^{\text{ML}}(\text{AND})$  is the minimum CIC achieved by a  $k$ -round memoryless quantum protocol computing AND with error at most  $\varepsilon$  on input distribution  $\mathcal{U}_0$ .

**Theorem 1.** *For any  $\varepsilon \in (0, 1/2)$  and any integer  $k$ ,  $\text{CIC}_{\mathcal{U}_0, \varepsilon, k}^{\text{ML}}(\text{AND}) = \Theta_\varepsilon\left(\frac{\log(k)}{k}\right)$ .*

The upper bound in Theorem 1 comes from a protocol described in [5] credited to Jain, Radhakrishnan and Sen. Note also that from [18], we could obtain a non-optimal bound of  $\text{CIC}_{\mathcal{U}_0, \varepsilon, k}^{\text{ML}}(\text{AND}) = \Omega_\varepsilon(1/k)$ , since the information-theoretic notion used in [18] becomes equivalent to CIC for memoryless protocols.

The question is then whether we can lift the lower bound of Theorem 1 to memoryless quantum protocols for DISJ. The obvious way to try and do it is to start with a memoryless quantum protocol for DISJ and use it in order to construct a memoryless protocol for AND. However, there is a problem. To solve AND, the players are given one-bit inputs, say  $x$  and  $y$ . But if they want to use a protocol solving DISJ over  $n$  bits, they need to create  $n - 1$  inputs for each party distributed in a way such that the protocol for DISJ will actually compute  $\text{AND}(x, y)$ . In the classical case, the players used private coins to choose the remaining inputs for DISJ, when we embed the AND function to it. In [18], the players used a superposition of coins in order to choose these inputs. Now, if the players keep these superpositions in their workspace, then we lose the memoryless property of our protocols. On the other hand, if they send these superpositions to the other player, the information cost of the protocol might considerably increase.

Since it is not obvious how to reduce DISJ to AND while retaining the memoryless property, similarly to the classical case where we do not know how to perform the reduction without the use of private coins, we slightly enhance our model to try to allow for this reduction to go through.

More precisely, we look at the model where the players do not possess any memory and hence they do not keep anything in their private space apart from their classical input *and* some classical private coins. Note that one can also assume the players share public coins without changing the model. In the classical case, we do allow for private coins when we define the information cost of a protocol. In the quantum case, note that we cannot unitarily create classical coins. Allowing classical coins seems like a minimal addition to the model. One can see that the communication complexity in this new model is not different from the communication complexity in the model without coins. Indeed, any protocol with coins can be simulated by a protocol where the coins are created in superposition by the players without changing the communication cost. But what about the information complexity? One one hand, the information complexity cannot increase, since we can always ignore the coins. Surprisingly, we show that it becomes as small as it can possibly be, namely, it equals the information revealed just by the value of the function. In other words, we say that any function can be computed privately. In fact, we show that every quantum protocol can be turned into a quantum protocol with coins that has the same input-output behaviour as the original protocol and that is perfectly private, i.e. the players only learn the value of the function the protocol computes and nothing more.

**Theorem 2.** *For every quantum communication protocol  $\Pi$ , there exists a memoryless quantum protocol  $\Pi'$  with private classical coins such that:*

- *on every input pair  $(x, y)$ ,  $\Pi'$  has the same output distribution as  $\Pi$ .*
- *the information cost of  $\Pi'$  is only the information gained by Bob's output  $\Pi_{\text{out}}$  in  $\Pi$ . This means that for every input distribution  $\mu$ , we have  $\text{CIC}_\mu(\Pi') = I(\Pi_{\text{out}}(X, Y) : X|Y)$ ,*

*where  $(X, Y)$  is a random variable distributed according to  $\mu$ ,  $I$  denotes the (classical) conditional mutual information and  $\Pi_{\text{out}}(x, y)$  is the (classical) random variable corresponding to Bob's output in  $\Pi$  on input  $(x, y)$ .*

Although we call the protocol  $\Pi'$  private, note that we are not interested in a cryptographic scenario where the players might deviate from the protocol: we are interested in studying the information of fixed protocols. In high level, in protocol  $\Pi'$  Alice and Bob follow  $\Pi$  but they use private coins to encrypt their messages. At the end of the protocol, if their coins were the same, Bob is able to output as in  $\Pi$  and knows nothing else than this value. However, if their coins were different, our construction prevents them from getting any information about each other's input, in which case they just restart the process until they get the same coins. This construction yields a private protocol at the expense of a very high communication cost.

Our results imply that given any function  $f$ , if we take for  $\Pi$  the protocol where Alice just sends over  $x$  to Bob who computes and output  $f(x, y)$ , we obtain a protocol  $\Pi'$  that can perfectly compute  $f$  with CIC only the information gained from  $f(x, y)$ .

**Corollary 3.** *For every input distribution  $\mu$ , and every positive integer  $k$ ,  $\text{CIC}_{\mu,k}^{\text{ML},\text{C}}(f) = I(f(X,Y) : X|Y)$ , where  $(X,Y)$  is a random variable distributed according to  $\mu$ ,  $I$  denotes the (classical) conditional mutual information, and  $\text{CIC}_{\mu,k}^{\text{ML},\text{C}}(f)$  denotes the minimum CIC achieved by a  $k$ -round memoryless quantum protocol with private classical coins to compute  $f$  exactly on input distribution  $\mu$ .*

Note that, in the case of AND, on distribution  $\mathcal{U}_0$  the output of  $\text{AND}(x,y) = x \wedge y$  is always 0. Hence, by the above result,  $\text{CIC}_{\mathcal{U}_0,k}^{\text{ML},\text{C}}(\text{AND}) = 0$  for every integer  $k$ .

There are two sides to this result. On the one hand, adding classical coins to quantum protocols allows for perfectly private protocols. This is impossible in the classical world and shows how quantum communication can offer advantages over classical communication. On the other hand, allowing the players to use private coins without restrictions weakens the power of information complexity as a lower bound for quantum protocols.

In order to try and salvage the notion of information complexity as a strong lower bound while allowing the players to use private coins, we consider an intermediate model where the players are allowed to use what we call *one-shot coins*. These are private coins that can be used only once during the protocol (then the players forget them). In the classical setting, this assumption is not restrictive and does not change the communication complexity nor the information complexity: for every protocol with private coins, we can construct a protocol which has the same transcript and output behaviours and uses only one-shot coins. This construction is done by changing only the way the coins are used [24].

In the quantum setting, this is not the case: allowing general coins or one-shot coins can lead to very different information complexities. We, in fact, show that one-shot coins do not necessarily decrease the information cost of a general quantum protocol by much. More precisely, we denote by  $\text{CIC}_{\mu,\epsilon,k}^{\text{ML},\text{C}_1}(f)$  the minimum CIC achieved by a  $k$ -round memoryless quantum protocol with private one-shot coins that computes  $f$  with error  $\epsilon$  on input distribution  $\mu$ , and prove that

**Theorem 4.** *For every  $k$ -round memoryless quantum protocol  $\Pi$  with one-shot coins, we can construct a  $k$ -round memoryless protocol  $\Pi'$  without coins, which has the same behaviour distribution as  $\Pi$  and such that  $\text{CIC}_{\mathcal{U}_0}(\Pi') = O(\text{CIC}_{\mathcal{U}_0}(\Pi) \cdot (\log(k) + |\log \text{CIC}_{\mathcal{U}_0}(\Pi)|))$ .*

Informally, the proof will go as follows. We will transform a memoryless quantum protocol  $\Pi$  with one-shot coins into a memoryless quantum protocol  $\Pi'$  without any coins, such that  $\Pi'$  will have the same outputs than  $\Pi$  and without increasing the information cost too much. The transformation from  $\Pi$  to  $\Pi'$  will informally be the following:

1. Quantize the coins from  $\Pi$  *i.e.*, put them in quantum superposition in quantum registers.
2. At each odd (or even) round, Alice (or Bob) applies the same transformation as in  $\Pi$ . Then, Alice (or Bob) would like to send all their quantum registers, including the coin registers, to the other player. Before doing that, Alice (or Bob) applies a compensation unitary that will limit the information cost increase that occurs because of the sending of all the quantum registers.

This result, combined with Theorem 1, implies in particular that  $\text{CIC}_{\mathcal{U}_0,\epsilon,k}^{\text{ML},\text{C}_1}(\text{AND}) = \Theta_\epsilon\left(\frac{1}{k}\right)$ . We see that while private coins allow for private protocols, one-shot coins not always do. The main open question is whether one-shot coins can be useful to reduce DISJ to AND or more generally prove some direct sum property for quantum information complexity.

## 2 Preliminaries

### 2.1 Quantum Communication

In the sequel we consider quantum protocols with classical inputs as defined in Figure 1. At the end of the protocol, Bob applies a measurement (POVM) on register  $\mathcal{O}$  to obtain a classical output.

Let  $k$  be an odd positive integer. A  $k$ -round protocol can be described as follows. At the outset of the protocol, Alice and Bob receive a classical input, in registers  $X$  and  $Y$  respectively. They will not modify the content of these registers. Alice starts with empty private memory and message registers,  $A_0$  and  $M_0$  respectively; Bob starts with an empty private memory register  $B_0$ . At each odd round  $1 \leq i \leq k$ , Alice applies a unitary operation on her private memory register,  $A_i$ , and the message register,  $M_i$ . This operation is controlled by her (classical) input. She then sends  $M_i$  to Bob. At each even round  $i$ , Bob applies a unitary operation, controlled by his input, on his private memory register,  $B_i$ , and the message register,  $M_i$ , and then sends  $M_i$  to Alice. After round  $k$  (Bob has just received message  $M_k$  from Alice since  $k$  is odd), Bob applies

a unitary  $U_{k+1}$  and measures part of his registers to obtain a classical output. For simplicity, let us denote  $B_{k+1} = U_{k+1}(B_k M_k)$ . We will split  $B_{k+1}$  into registers  $\mathcal{G}_B$  and  $\mathcal{O}$  such that the part of  $B_{k+1}$  that is measured by Bob at the end is  $\mathcal{O}$ .

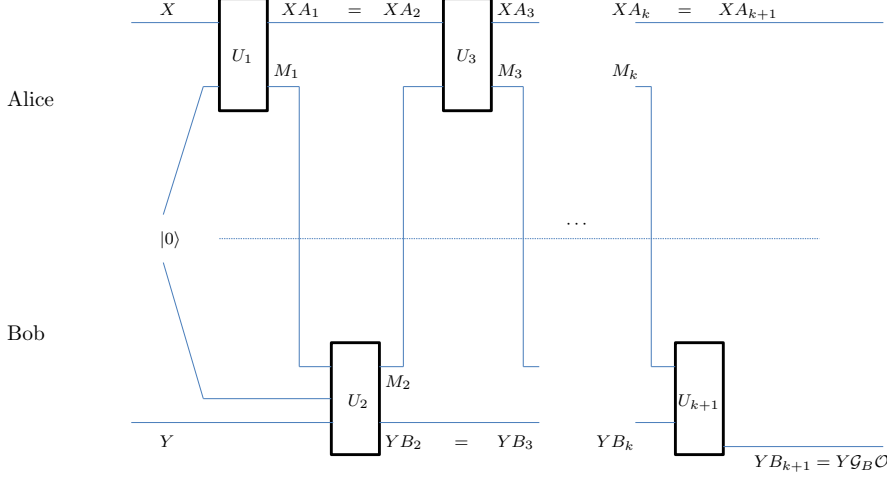


Figure 1: Depiction of a quantum protocol with classical inputs in the interactive model, adapted from the long version of [27, Figure 1]. The local operations  $U_i$  are unitary operators. The  $A_i$  registers are Alice's local memory in round  $i$ , similarly the  $B_i$ 's are Bob's, the  $M_i$ 's are the message registers, exchanged back-and-forth between them.  $X$  and  $Y$  are Alice's and Bob's respective input, distributed according to some prior  $\mu$ .

**Definition 5** (Quantum communication complexity). *The quantum communication cost of a quantum protocol  $\Pi$  is:  $\text{QCC}(\Pi) = \sum_i \log \dim(M_i)$ , where  $M_i$  is the quantum register that corresponds to the message sent over at round  $i$ .*

*For a fixed function  $f$ , the average-case quantum communication complexity of  $f$  relative to input distribution  $\mu$  and with (distributional) error  $\epsilon \in [0, 1]$  is defined as*

$$\text{QCC}_{\mu, \epsilon}(f) = \inf_{\Pi} \text{QCC}(\Pi)$$

*where the infimum is taken over all protocols  $\Pi$  computing  $f$  with average error at most  $\epsilon$  with respect to input distribution  $\mu$ . The worst-case quantum communication complexity of  $f$  with error  $\epsilon$  is defined as*

$$\text{QCC}_{\epsilon}(f) = \inf_{\Pi} \text{QCC}(\Pi)$$

*where the infimum is taken over all protocols  $\Pi$  computing  $f$  with worst-case error at most  $\epsilon$ .*

## 2.2 The Classical Input Information Cost (CIC) of quantum protocols

Let us recall the usual definition of information cost in classical protocols (see e.g. [12, 4]). The information cost of a protocol  $\Pi$  is the amount information revealed by the whole transcript of  $\Pi$ , that is, the messages and the public coins. For simplicity, we also denote  $\Pi$  the random variable corresponding to the transcript of  $\Pi$  on input  $X, Y$ . Then we have

$$\text{IC}(\Pi) = I(X : \Pi | Y, R_B) + I(Y : \Pi | X, R_A).$$

By a chain rule argument, it is possible to rewrite IC as the sum over the rounds of the information that the receiver of a message learns about the input of the other player, conditioned on what he already knew before receiving the message (that is, the information contained in his input and the past messages).

**Definition 6** (Information cost). *The information cost of a (randomized) classical protocol  $\Pi$ , over input distribution  $\mu$ , is*

$$\text{IC}(\Pi) = \sum_{i: \text{odd}} I(M_i : X|Y, R_B, M_{[i-1]}) + \sum_{i: \text{even}} I(M_i : Y|X, R_A, M_{[i-1]}),$$

where  $M_{[i-1]} = M_1, \dots, M_{i-1}$  is the concatenation of all messages sent before round  $i$ .

For a fixed function  $f$  the information complexity of  $f$  relative to input distribution  $\mu$  and with (distributional) error  $\epsilon \in [0, 1]$  is defined as  $\text{IC}_{\mu, \epsilon}(f) = \inf_{\Pi} \text{IC}_{\mu}(\Pi)$  where the infimum is taken over all protocols  $\Pi$  computing  $f$  with error at most  $\epsilon$  with respect to  $\mu$ .

Imitating this round-by-round definition of IC, [20] introduced a version of information cost for quantum protocols with classical inputs. It is the sum of the information that the message receiver learns about the sender's (classical) input at each round, conditioned on the registers held by the receiver.

In the sequel, for a quantum state  $\rho^{A,B,C}$  over registers  $A, B$  and  $C$  (i.e.  $A, B, C$  are three disjoint finite dimensional quantum systems having some joint density matrix  $\rho$ ), we denote by  $\rho_A = \text{Tr}_{BC}(\rho)$  the reduced density matrix of  $A$  and by  $S(A) = -\text{Tr}(\rho_A \log(\rho_A))$  the von Neumann entropy of  $A$ .  $I(A : B) = S(A) + S(B) - S(AB)$  denotes the quantum mutual information between  $A$  and  $B$  and  $I(A : B|C) = I(A : B, C) - I(A : C)$  is the quantum condition mutual information between registers  $A$  and  $B$  conditioned on  $C$ .

With the notations introduced above for quantum protocols, this leads to the following definition.

**Definition 7** (Classical input information complexity [20]). *The classical input information cost of a quantum protocol  $\Pi$  over input distribution  $\mu$  is:*

$$\text{CIC}_{\mu}(\Pi) = \sum_{i: \text{odd}} I(M_i : X|Y, B_i) + \sum_{i: \text{even}} I(M_i : Y|X, A_i).$$

For a fixed function  $f$  the classical input quantum information complexity of  $f$  relative to input distribution  $\mu$  and with (distributional) error  $\epsilon \in [0, 1]$  is defined as

$$\text{CIC}_{\mu, \epsilon}(f) = \inf_{\Pi} \text{CIC}_{\mu}(\Pi)$$

where the infimum is taken over all protocols  $\Pi$  computing  $f$  with error at most  $\epsilon$  with respect to  $\mu$ .

Touchette [27] has defined a different notion of quantum information cost (QIC), but as shown in [24], QIC and CIC are equivalent within a factor of 2. In fact, for memoryless protocols QIC is exactly two times CIC, and hence we only look at CIC in the rest of the paper.

### 2.3 Measures of distance between quantum states

Let us recall a few tools about classical-quantum states and measures of distance between two quantum states. If  $C$  is a classical random variable taking the classical value  $|c\rangle$  with probability  $p_c$ , then  $I(A : B|C) = \sum_c p_c I(A^c : B^c)$ , where  $(AB)^c$  denotes the joint density matrix of  $A$  and  $B$  when  $C = |c\rangle$ . We also write  $I(A : B|C = c)$  for  $I(A^c : B^c)$ .

**Definition 8.** Let  $\rho$  and  $\sigma$  be density matrices in the same finite dimensional Hilbert space. The trace distance between  $\rho$  and  $\sigma$  is defined as  $\Delta(\rho, \sigma) = \frac{1}{2} \text{Tr} \left( \sqrt{(\rho - \sigma)^{\dagger}(\rho - \sigma)} \right)$ , where  $\dagger$  denotes the conjugate-transposition.

We recall that  $\Delta$  is preserved under unitary transformations: for every unitary operator  $U$ , and every  $\rho$  and  $\sigma$  as above,  $\Delta(U\rho U^{\dagger}, U\sigma U^{\dagger}) = \Delta(\rho, \sigma)$ . When the states are pure, say  $\rho = |\psi\rangle\langle\psi|$  and  $\sigma = |\phi\rangle\langle\phi|$ , then

$$\Delta(\rho, \sigma) = \frac{1}{2} \sqrt{1 - |\langle\psi|\phi\rangle|^2}. \quad (1)$$

**Definition 9.** Let  $\rho$  and  $\sigma$  be density matrices in the same finite dimensional Hilbert space  $H$ . The fidelity (also called Bhattacharyya coefficient) between  $\rho$  and  $\sigma$  is defined as  $F(\rho, \sigma) = \text{Tr} \left( \sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} \right)$ .

By Uhlmann's theorem, we also have the following characterization:  $F(\rho, \sigma) = \sup_{K, |\phi\rangle, |\psi\rangle} |\langle\phi|\psi\rangle|$ , where the maximization is over Hilbert space  $K$  and purification  $|\phi\rangle$  and  $|\psi\rangle$  in  $H \otimes K$  of  $\rho$  and  $\sigma$  respectively. We will make use of the following result.

**Lemma 10** (see e.g. [25]). Let  $\rho$  and  $\sigma$  be density matrices in the same finite dimensional Hilbert space  $H$ . Let  $E = \{E_m\}_m$  be a POVM on  $H$ . Let  $p_m = \text{Tr}(\rho E_m)$  and  $q_m = \text{Tr}(\sigma E_m)$ . We have  $\Delta(\rho, \sigma) \geq \frac{1}{2} \sum_m |p_m - q_m|$ .

## 2.4 Memoryless quantum communication

A particular class of quantum communication protocols are those where the players send back and forth the message register without keeping any information in their private memory register apart from their classical input.

**Definition 11.** *A quantum communication protocol is said to be a memoryless protocol if and only if the following condition is satisfied: the players' private registers, namely  $A_i, B_i$  (see Fig. 1), are always empty, meaning that their working registers correspond only to the message registers. This implies that at each round, the sender will always send all the registers he or she currently has except the input register to the other player.*

While at first hand, this family of protocols seems restricted, since messages can not be entangled with private memory registers (nor with the environment), they constitute a powerful and worth-studying class of protocols. As we have said in Section 1, almost all quantum protocols we know are memoryless. Moreover, there is a deep connection between memoryless protocols and Bell inequality violations and such protocols can be much easier to implement. Last but not least, we will see in the following sections that it is easier to understand the flow of quantum information in memoryless protocols, for example, the information that is learnt in the protocol is exactly the same as the information been forgotten.

Let us denote by  $\mathcal{T}_{\mu, \epsilon, k}^{\text{ML}}(f)$  the set of all  $k$ -round memoryless protocols  $\Pi$  computing function  $f$  with error at most  $\epsilon$  with respect to  $\mu$ .

**Definition 12.** *The  $k$ -round  $\epsilon$ -error memoryless quantum communication complexity of a function  $f$  relative to input distribution  $\mu$  is defined as  $\text{QCC}_{\mu, \epsilon, k}^{\text{ML}}(f) = \inf_{\Pi \in \mathcal{T}_{\mu, \epsilon, k}^{\text{ML}}(f)} \text{QCC}_{\mu}(\Pi)$ .*

**Definition 13.** *The  $k$ -round  $\epsilon$ -error memoryless classical input information complexity of  $f$  relative to input distribution  $\mu$  is defined as  $\text{CIC}_{\mu, \epsilon, k}^{\text{ML}}(f) = \inf_{\Pi \in \mathcal{T}_{\mu, \epsilon, k}^{\text{ML}}(f)} \text{CIC}_{\mu}(\Pi)$ .*

In [18], the authors used a notion of quantum information loss (denoted QIL here) of a protocol  $\Pi$ , defined, with the notation introduced above, by:

$$\text{QIL}_{\mu, \epsilon, k}(\Pi) = \sum_{i: \text{odd}} I(X : M_i B_i | Y) + \sum_{i: \text{even}} I(Y : M_i A_i | X).$$

For memoryless protocols, private memory registers  $A$  and  $B$  are empty, so this notion coincides with the notion of classical input information cost (CIC).

## 3 The CIC of bounded-round memoryless protocols for AND

In this section, we prove the following result, where  $\mathcal{U}_0$  denotes the uniform distribution over  $\{(0, 0), (0, 1), (1, 0)\}$ .

**Theorem 1.** *For any  $\epsilon \in (0, 1/2)$  and any integer  $k$ ,  $\text{CIC}_{\mathcal{U}_0, \epsilon, k}^{\text{ML}}(\text{AND}) = \Theta_{\epsilon} \left( \frac{\log(k)}{k} \right)$ .*

This is a consequence of our lower bound in Proposition 18 and the upper bound in [18, 5] (see Section 3.3).

### 3.1 Optimal lower bound for the information cost of a pure message

We first study the information cost of a single quantum message which is in a pure state. Let us recall that, using Pinsker's inequality, we have the following result.

**Lemma 14** (see [14]). *Suppose  $X$  and  $Q$  are disjoint quantum systems, where  $X$  is a classical random variable uniformly distributed over  $\{0, 1\}$  and  $Q$  is a quantum encoding  $x \rightarrow \sigma_x$  of  $X$ . Then, the following relationship holds between mutual information and fidelity:*

$$I(X : Q) \geq 1 - F(\sigma_0, \sigma_1).$$

In the sequel, for a quantum state  $Q$  depending on classical inputs in  $\mathbf{X} \times \mathbf{Y}$ , we denote by  $Q^{x,y}$  the value of  $Q$  when the inputs are  $(x, y)$ . The above result leads to the following corollary, which applies to the general situation where  $M$  is a quantum message which is non necessarily in a pure state.

**Corollary 15.** *Let  $X, Y$  be two classical random variables taking value in  $\{0, 1\}$ . Let  $M$  be a quantum encoding of  $(X, Y)$ . Then  $I(X : M | Y = y) \geq 1 - F(M^{1y}, M^{0y})$ .*

In this section, we prove a tighter inequality (i.e. a larger lower bound) that holds when  $M$  is a pure state. Let  $h_2$  be the binary entropy function:  $h_2 : [0, 1] \rightarrow [0, 1]$ ,  $p \mapsto -p \log p - (1-p) \log(1-p)$  where  $\log$  denotes the base 2 logarithm, with the convention that  $0 \log 0 = 0$ , and let  $h_2^{-1}$  be its inverse function from  $[0, 1]$  to  $[0, 0.5]$ .

**Lemma 16.** *Consider the bipartite quantum state over two registers,  $X$  and  $M$ ,  $\rho = \sum_{x \in \{0,1\}} \frac{1}{2} |x\rangle \langle x|_X \otimes |\psi_x\rangle \langle \psi_x|_M$ , for some pure states  $|\psi_x\rangle$ ,  $x = 0, 1$ . Then*

$$I(X : M) = h_2 \left( \frac{1 - |\langle \psi_0 | \psi_1 \rangle|}{2} \right).$$

*Proof.* Let  $\delta \in [0, 1]$  and  $\alpha \in (-\pi/2, \pi/2]$  such that  $\cos(\alpha) = 1 - \delta = |\langle \psi_0 | \psi_1 \rangle|$ . We have

$$\begin{aligned} I(X : M) &= S(X) + S(M) - S(XM) \\ &= 1 + S \left( \frac{1}{2} |\psi_0\rangle \langle \psi_0| + \frac{1}{2} |\psi_1\rangle \langle \psi_1| \right) - S \left( \frac{1}{2} |0\rangle \langle 0| \otimes |\psi_0\rangle \langle \psi_0| + \frac{1}{2} |1\rangle \langle 1| \otimes |\psi_1\rangle \langle \psi_1| \right) \\ &= S \left( \frac{1}{2} |\psi_0\rangle \langle \psi_0| + \frac{1}{2} |\psi_1\rangle \langle \psi_1| \right). \end{aligned}$$

Let  $N, N' > 0$  such that  $|\psi_+\rangle = \frac{1}{N}(|\psi_0\rangle + |\psi_1\rangle)$  and  $|\psi_-\rangle = \frac{1}{N'}(|\psi_0\rangle - |\psi_1\rangle)$  are of norm 1. We have

$$\begin{aligned} \frac{1}{2} |\psi_0\rangle \langle \psi_0| + \frac{1}{2} |\psi_1\rangle \langle \psi_1| &= \cos^2 \left( \frac{\alpha}{2} \right) |\psi_+\rangle \langle \psi_+| + \sin^2 \left( \frac{\alpha}{2} \right) |\psi_-\rangle \langle \psi_-| \\ &= \left( 1 - \frac{\delta}{2} \right) |\psi_+\rangle \langle \psi_+| + \frac{\delta}{2} |\psi_-\rangle \langle \psi_-|. \end{aligned}$$

Since  $|\psi_+\rangle$  and  $|\psi_-\rangle$  are orthogonal, this gives :

$$I(X : M) = S \left( \frac{1}{2} |\psi_0\rangle \langle \psi_0| + \frac{1}{2} |\psi_1\rangle \langle \psi_1| \right) = S \left( \left( 1 - \frac{\delta}{2} \right) |\psi_+\rangle \langle \psi_+| + \frac{\delta}{2} |\psi_-\rangle \langle \psi_-| \right) = h_2(\delta/2).$$

□

**Corollary 17.** *Consider the bipartite quantum state  $\rho = \sum_{x \in \{0,1\}} \frac{1}{2} |x\rangle \langle x|_X \otimes |\psi_x\rangle \langle \psi_x|_M$ . We have  $I(X : M) \geq h_2 \left( \frac{1}{4} \Delta^2(|\psi_0\rangle, |\psi_1\rangle) \right)$ .*

*Proof.* From Lemma 16, we have  $I(X : M) \geq h_2 \left( \frac{1 - |\langle \psi_0 | \psi_1 \rangle|}{2} \right)$ . The conclusion holds since  $(1 - |\langle \psi_0 | \psi_1 \rangle|) \geq \frac{1}{2} \Delta^2(|\psi_0\rangle, |\psi_1\rangle)$  by (1), and  $h_2$  is increasing on  $[0, 0.5]$ . □

As a consequence, when the state is tripartite  $\rho = \sum_{x,y \in \{0,1\}} \frac{1}{4} |x\rangle \langle x|_X \otimes |\psi_{x,y}\rangle \langle \psi_{x,y}|_M \otimes |y\rangle \langle y|_Y$ , we obtain

$$I(X : M|Y = y) \geq h_2 \left( \frac{1}{4} \Delta^2(|\psi_{0,y}\rangle, |\psi_{1,y}\rangle) \right),$$

instead of the bound given by Corollary 15.

### 3.2 Optimal lower bound for the information cost of bounded-round memoryless quantum protocols for AND

We show the following result. The proof is very similar to the one presented in [18] and the improvement we obtain relies on Corollary 17.

**Proposition 18.**  $\text{CIC}_{\mathcal{U}_0, \epsilon, k}^{\text{ML}}(\text{AND}) \geq \frac{1}{12k} (1 - 2\epsilon)^2 \log(k) = \Omega(\log(k)/k)$ .

In the proof, it will be easier to study the following quantity, defined for every  $k$ -round memoryless quantum protocol  $\overline{\Pi}$  :

$$\text{CIC}_{\mu}^0(\overline{\Pi}) = \sum_{i=1, \text{ odd}}^k I(M_i : X|Y = 0) + \sum_{i=1, \text{ even}}^k I(M_i : Y|X = 0).$$

It is tightly related to the classical input information cost under distribution  $\mathcal{U}_0$ .



**Lemma 19.**  $\text{CIC}_{\mathcal{U}_0, \epsilon, k}^{\text{ML}}(\text{AND}) = \inf_{\bar{\Pi}} \text{CIC}_{\mathcal{U}_0}(\bar{\Pi}) = \frac{2}{3} \inf_{\bar{\Pi}} \text{CIC}_{\mathcal{U}_0}^0(\bar{\Pi})$ , where the infimum is over memoryless  $k$ -round protocols computing AND with error at most  $\epsilon$  with respect to  $\mathcal{U}_0$ .

*Proof.* Let us consider such a protocol  $\bar{\Pi}$  and denote  $M_i$  its  $i$ -th message ( $1 \leq i \leq k$ ). We have

$$\text{CIC}_{\mathcal{U}_0}(\bar{\Pi}) = \sum_{i: \text{odd}} I(M_i : X|Y) + \sum_{i: \text{even}} I(M_i : Y|X).$$

Moreover, under distribution  $\mathcal{U}_0$ , for any odd  $i \leq k$ ,

$$\begin{aligned} I(M_i : X|Y) &= \mathbb{P}(Y=0)I(M_i : X|Y=0) + \mathbb{P}(Y=1)I(M_i : X|Y=1) \\ &= \frac{2}{3}I(M_i : X|Y=0), \end{aligned}$$

since, when  $Y=1$ ,  $X=0$  with probability 1 so  $I(M_i : X|Y=1)=0$ . Similarly, for any even  $i$ ,

$$I(M_i : Y|X) = \frac{2}{3}I(M_i : Y|X=0).$$

From this, we conclude the lemma.  $\square$

We now prove Proposition 18.

*Proof of Proposition 18.* By Lemma 19, it suffices to show that for every  $k$ -round memoryless protocol  $\bar{\Pi}$ ,

$$\text{CIC}_{\mathcal{U}_0}^0(\bar{\Pi}) \geq \frac{(1-2\epsilon)^2 \log(k)}{8k}.$$

Consider such a memoryless protocol  $\bar{\Pi}$ . It can be described with the following notations. Alice and Bob have respective inputs  $x$  and  $y$ . Alice starts with  $|0\rangle = |\psi_{xy}^0\rangle$ . At odd (resp. even) round  $i$ , Alice (resp. Bob) sends a message. For each  $i \leq k$ , let us denote  $|\psi_{x,y}^i\rangle$  the state of the message register just after it has been sent over. We assume that the last message is sent by Alice to Bob (*i.e.*,  $k$  is odd).

For simplicity, let us define, for  $i \leq k$ ,

$$a_i = \begin{cases} I(M_i : X|Y=0) & \text{if } i \text{ is odd,} \\ I(M_i : Y|X=0) & \text{if } i \text{ is even.} \end{cases}$$

So  $\text{CIC}_{\mathcal{U}_0}^0(\bar{\Pi}) = \sum_{i=1}^k a_i$ . For  $i \leq k$ , we also define

$$b_i = \begin{cases} \Delta(|\psi_{10}^i\rangle, |\psi_{00}^i\rangle) & \text{if } i \text{ is odd,} \\ \Delta(|\psi_{01}^i\rangle, |\psi_{00}^i\rangle) & \text{if } i \text{ is even,} \end{cases}$$

and

$$\delta_i = \begin{cases} \Delta(|\psi_{01}^i\rangle, |\psi_{11}^i\rangle) & \text{if } i \text{ is odd,} \\ \Delta(|\psi_{10}^i\rangle, |\psi_{11}^i\rangle) & \text{if } i \text{ is even.} \end{cases}$$

We first prove three claims.

**Claim 20.** *It holds that  $\delta_k \geq 1 - 2\epsilon$ .*

*Proof.* For any inputs  $(x, y)$ , Bob outputs  $x \wedge y$  with probability at least  $1 - \epsilon$  at the end of the protocol, where he has the state  $|\psi_{xy}^k\rangle$ . In particular, on inputs  $(1, 0)$ , Bob will output 0 with probability  $1 - \epsilon$  and on inputs  $(1, 1)$ , Bob will output 1 with probability  $1 - \epsilon$ . The conclusion holds by Lemma 10 and by the fact that  $\delta_k = \Delta(|\psi_{01}^k\rangle, |\psi_{11}^k\rangle)$ .  $\square$

**Claim 21.** *It holds that  $\delta_k \leq 2 \sum_{i=1}^k b_i$ .*

*Proof.* Let us first notice that for every  $i \leq k$ ,  $\delta_i \leq b_{i-1} + b_i + \delta_{i-1}$ . Indeed, if  $i$  is odd,

$$\begin{aligned} \delta_i &= \Delta(|\psi_{01}^i\rangle, |\psi_{11}^i\rangle) \\ &\leq \Delta(|\psi_{01}^i\rangle, |\psi_{00}^i\rangle) + \Delta(|\psi_{00}^i\rangle, |\psi_{10}^i\rangle) + \Delta(|\psi_{10}^i\rangle, |\psi_{11}^i\rangle) && \text{(by triangle inequality)} \\ &\leq \Delta(|\psi_{01}^{i-1}\rangle, |\psi_{00}^{i-1}\rangle) + b_i + \Delta(|\psi_{10}^{i-1}\rangle, |\psi_{11}^{i-1}\rangle) && \text{(by unitary invariance of } \Delta) \\ &= b_{i-1} + b_i + \delta_{i-1}, \end{aligned}$$

where the second inequality holds since, at round  $i$ , Alice is the sender, and the unitary she applies depend only on her input (which is  $x = 0$  for both  $|\psi_{01}^i\rangle$  and  $|\psi_{00}^i\rangle$ , and  $x = 1$  for both  $|\psi_{10}^i\rangle$  and  $|\psi_{11}^i\rangle$ ). We repeat a similar argument if  $i$  is even. Then, Claim 21 is obtained by repeating this in a recursive way down to  $i = 1$ .  $\square$

**Claim 22.** *If for all  $i \leq k$  we have  $a_i \leq 0.4$ , then  $\sum_{i=1}^k b_i \leq 2k\sqrt{h_2^{-1}\left(\frac{\text{CIC}_{\mathcal{U}_0}^0(\bar{\Pi})}{k}\right)}$ .*

*Proof.* Let us assume that for all  $i \leq k$  we have  $a_i \leq 0.4$ . By Corollary 17, we have for all  $i \leq k$  that  $b_i \leq 2\sqrt{h_2^{-1}(a_i)}$ , hence

$$\sum_{i=1}^k b_i \leq \sum_{i=1}^k 2\sqrt{h_2^{-1}(a_i)}.$$

We can check analytically that the function  $f : x \mapsto 2\sqrt{h_2^{-1}(x)}$  is concave on the interval  $[0, 0.4]$ . Since, by assumption,  $a_i$  lies in this interval for all  $i \leq k$ , we have by concavity of  $f$ :

$$\sum_{i=1}^k b_i \leq \sum_{i=1}^k 2\sqrt{h_2^{-1}(a_i)} = k \sum_{i=1}^k \frac{1}{k} 2\sqrt{h_2^{-1}(a_i)} \leq 2k\sqrt{h_2^{-1}\left(\frac{\text{CIC}_{\mathcal{U}_0}^0(\bar{\Pi})}{k}\right)}.$$

$\square$

We now conclude the proof of Proposition 18. If there exists  $j \leq k$  such that  $a_j > 0.4$ , then we immediately have

$$\text{CIC}_{\mathcal{U}_0}^0(\bar{\Pi}) = \sum_{i=1}^k a_i \geq a_j > 0.4 \geq \frac{(1-2\varepsilon)^2 \log(k)}{8k}.$$

We now consider the case where  $a_i \leq 0.4$  for all  $i \leq k$ . We combine Claims 20, 21 and 22 to obtain

$$\frac{1}{2}(1-2\varepsilon) \leq 2k\sqrt{h_2^{-1}\left(\frac{\text{CIC}_{\mathcal{U}_0}^0(\bar{\Pi})}{k}\right)},$$

which implies

$$\frac{\text{CIC}_{\mathcal{U}_0}^0(\bar{\Pi})}{k} \geq h_2\left(\frac{(1-2\varepsilon)^2}{16k^2}\right).$$

From there, we obtain, using the fact that  $h_2(x) \geq x \log(1/x)$  for any  $x \in [0, 1]$ :

$$\frac{\text{CIC}_{\mathcal{U}_0}^0(\bar{\Pi})}{k} \geq h_2\left(\frac{(1-2\varepsilon)^2}{16k^2}\right) \geq \frac{(1-2\varepsilon)^2}{16k^2} \log\left(\frac{16k^2}{(1-2\varepsilon)^2}\right) \geq \frac{(1-2\varepsilon)^2 \log(k)}{8k^2}.$$

This yields  $\text{CIC}_{\mathcal{U}_0}^0(\bar{\Pi}) \geq \frac{(1-2\varepsilon)^2 \log(k)}{8k}$ . We conclude the proof of Proposition 18 using Lemma 19.  $\square$

### 3.3 Tightness of the bound

In [5], the authors provide a protocol, denoted here  $\Pi_{\text{AND}}$  and described at Figure 2, attributed to Jain, Radhakrishnan and Sen. It was proved to compute AND correctly under the distribution  $\mathcal{U}_0$  and to have information cost  $O(\log(k)/k)$ .

Since  $\Pi_{\text{AND}}$  does not use any private memory register, their result and the lower bound provided by Proposition 18 yield Theorem 1.

**Protocol  $\Pi_{\text{AND}}$ .** Inputs :  $(x, y) \in \{0, 1\} \times \{0, 1\}$ . Parameter  $r \in \mathbb{N}$ .

1. Set  $\theta = \frac{\pi}{8r}$ . Let  $|v\rangle$  be the vector  $\cos(\theta)|0\rangle + \sin(\theta)|1\rangle$ . Let  $U_v$  be the unitary operation of reflecting about the vector  $|v\rangle$  i.e.  $U_v|0\rangle = \cos(2\theta)|0\rangle + \sin(2\theta)|1\rangle$  and  $U_v|1\rangle = \sin(2\theta)|0\rangle - \cos(2\theta)|1\rangle$ . Also let  $Z$  be the unitary operation of reflecting about  $|0\rangle$ , i.e.  $Z|0\rangle = |0\rangle$  and  $Z|1\rangle = -|1\rangle$ .
2. Alice starts by preparing a qubit  $C$  in state  $|0\rangle$ .
3. If  $x = 0$ , Alice applies the identity operation on  $C$  and sends it to Bob. If  $x = 1$ , Alice applies the  $U_v$  operation on  $C$  and sends it to Bob.
4. If  $y = 0$ , Bob applies the identity operation on  $C$  and sends it to Alice. If  $y = 1$ , Bob applies the  $Z$  operation on  $C$  and sends it to Alice.
5. After  $k = 4r - 1$  rounds, Bob measures the register  $C$ . If the result is 1, then he answers 1, otherwise he answers 0. He also sends this to Alice.

Figure 2: Quantum protocol for AND.

## 4 Classical coins allow for private quantum protocols

In this section, we study the behavior of CIC when the players are allowed to have private classical coins. We show that we can transform any quantum protocol into a memoryless quantum protocol with private coins whose CIC is exactly the information Bob learns just from the output of the protocol and nothing more.

Let us denote by  $\mathcal{T}_{\mu, \epsilon, k}^{\text{ML}, \text{C}}(f)$  the set of all  $k$ -round memoryless protocols  $\Pi$  with private coins computing function  $f$  with error at most  $\epsilon$  with respect to  $\mu$ .

We define the following notions for CIC with private coins.

**Definition 23.** The  $k$ -round  $\epsilon$ -error private-coin memoryless classical input information complexity of  $f$  relative to input distribution  $\mu$  is defined as  $\text{CIC}_{\mu, \epsilon, k}^{\text{ML}, \text{C}}(f) = \inf_{\Pi \in \mathcal{T}_{\mu, \epsilon, k}^{\text{ML}, \text{C}}(f)} \text{CIC}_{\mu}(\Pi)$ . We also define the quantity  $\text{CIC}_{\mu, \epsilon, k}^{\text{C}}(f)$  where we remove the memoryless constraint.

Here, we will prove the following (restated) result.

**Theorem 2.** For every quantum communication protocol  $\Pi$ , there exists a memoryless quantum protocol  $\Pi'$  with private classical coins such that:

- on every input pair  $(x, y)$ ,  $\Pi'$  has the same output distribution as  $\Pi$ .
- the information cost of  $\Pi'$  is only the information gained by Bob's output  $\Pi_{\text{out}}$  in  $\Pi$ . This means that for every input distribution  $\mu$ , we have  $\text{CIC}_{\mu}(\Pi') = I(\Pi_{\text{out}}(X, Y) : X|Y)$ ,

where  $(X, Y)$  is a random variable distributed according to  $\mu$ ,  $I$  denotes the (classical) conditional mutual information and  $\Pi_{\text{out}}(x, y)$  is the (classical) random variable corresponding to Bob's output in  $\Pi$  on input  $(x, y)$ .

We say that such a protocol  $\Pi'$  is private since it leaks the minimal CIC possible: any protocol leaks at least as much information as Bob's output leaks to himself.

*Proof.* Let us consider a  $k$ -round quantum protocol  $\Pi$  where Alice and Bob respectively have classical input  $x$  and  $y$ . At the end of the protocol, Bob has an output in quantum register  $\mathcal{O}_B = \mathcal{O}_k$ , which he measures in the computational basis to get  $f(x, y)$ . Alice and Bob also share at the end of the protocol some garbage state in registers  $\mathcal{G}_A, \mathcal{G}_B$ . We have  $\mathcal{G}_A = A_k$  and  $\mathcal{G}_B = (B_k, \mathcal{O}_k) = (B_k, \mathcal{O}_B)$ .

If at the end of  $\Pi$  the output register  $\mathcal{O}_B$  contains a superposition and not a mixture, we consider that Bob has an additional register  $\mathcal{O}'_B$  and applies a CNOT operation on  $\mathcal{O}_B, \mathcal{O}'_B$ , so that  $\mathcal{O}_B$  is a mixture. Bob now uses  $\mathcal{O}_B$  as his output register. This protocol succeeds with the same probability as  $\Pi$ , so for notational simplicity we also denote it  $\Pi$ .

We now transform protocol  $\Pi$  into a protocol  $\bar{\Pi}$  which uses private classical coins and is a private protocol. In  $\bar{\Pi}$ , Alice and Bob will have some extra random coins. Let  $m = \sum_{i=1}^k |M_i|$ ,  $a = \sum_{i=1}^k |A_i|$ ,  $b = \sum_{i=1}^k |B_i|$  the

total number of qubits sent in  $\Pi$ , and the cumulated memory sizes used by Alice and Bob respectively. Let  $t = 2(m + a + b)$ . In  $\bar{\Pi}$ , we give Alice and Bob respectively  $t_A = (t_A^1, \dots, t_A^k)$  and  $t_B = (t_B^1, \dots, t_B^k)$  random coins, where  $t_A^1, t_B^1$  are of length  $2(|A_0| + |M_0|)$  and  $t_A^i, t_B^i$  are of length  $2(|M_i| + |A_i| + |B_i|)$ ,  $2 \leq i \leq r$ . We also give Bob extra randomness  $s_B$  of length  $2(|A_k| + |B_k| + |M_k|)$  and Alice extra randomness  $s_A$  of length  $2(|A_k| + |B_k| + |M_k| - 1)$ . The coins  $t_A$  and  $t_B$  will be used to perform an encrypted version of  $\Pi$  while the coins  $s_A, s_B$  will be used to retrieve the output with minimum information leakage.

Each player will encrypt the message he sends using the quantum one time pad. The quantum one time pad (QOTP) acting on  $q$  qubits is the unitary  $\mathcal{E}$  taking  $2q$  classical bits  $s = (s_1, \dots, s_{2q})$  as parameters such that

$$\mathcal{E}_s(|\phi\rangle) = \left( \bigotimes_{i=1}^q X^{s_{2i-1}} Z^{s_{2i}} \right) |\phi\rangle$$

where  $X$  and  $Z$  are respectively the bit flip operator and the phase flip operator. Note that the encrypted state when we average uniformly over  $s$  is the totally mixed state.

We can now present our protocol  $\bar{\Pi}$ :

**1. Alice and Bob perform an encrypted version of  $\Pi$  using coins  $t_A$  and  $t_B$ :**

- At round 1, Alice applies the same unitary  $U_1$  as in  $\Pi$  on registers  $A_0M_0$  to obtain  $A_1M_1$ . Then, she encrypts register  $A_1M_1$  by applying the QOTP  $\mathcal{E}_{t_A^1}$  on these registers. Finally, she sends  $A_1M_1$  to Bob.
- For  $i \in \{2, \dots, k\}$ ,
  - if  $i$  is even, Bob applies  $(\mathcal{E}_{t_B^{i-1}})^{-1}$  on register  $A_{i-1}M_{i-1}B_{i-1}$  ( $(\mathcal{E}_{t_B^1})^{-1}$  will act only on  $A_1M_1$ ) as an attempt to undo Alice's encryption. Bob then applies the same unitary  $U_i$  as in  $\Pi$  on registers  $M_{i-1}B_{i-1}$  to obtain  $M_iB_i$ . We have here  $A_i = A_{i-1}$ . Then, he encrypts registers  $A_iM_iB_i$  by applying the QOTP  $\mathcal{E}_{t_B^i}$  on these registers. Finally, he sends  $A_iM_iB_i$  to Alice.
  - if  $i$  is odd, Alice applies  $(\mathcal{E}_{t_A^{i-1}})^{-1}$  on register  $A_{i-1}M_{i-1}B_{i-1}$  as an attempt to undo Bob's encryption. Alice then applies the same unitary  $U_i$  as in  $\Pi$  on registers  $A_{i-1}M_{i-1}$  to obtain  $A_iM_iB_i$ . Here, we have  $B_i = B_{i-1}$ . Then, she encrypts registers  $A_iM_iB_i$  by applying the QOTP  $\mathcal{E}_{t_A^i}$  on these registers. Finally, she sends  $A_iM_iB_i$  to Bob.
- Finally, Bob applies  $(\mathcal{E}_{t_B^k})^{-1}$  on registers  $A_kM_kB_k$  as an attempt to undo Alice's encryption. Bob then applies  $U_{k+1}$  on register  $B_k = \mathcal{G}_B \mathcal{O}_B$  to get his output.

At this point, notice here that, if for all  $i = 1, \dots, k$ , we have  $t_A^i = t_B^i$ , then Alice and Bob essentially performed  $\Pi$ .

- 2. Bob sends his registers after encryption:** Bob applies  $\mathcal{E}_{s_B}$  on all the registers he holds, namely  $A_kM_kB_k$ , and sends them all to Alice.
- 3. Checking the coins  $t_A = t_B$ :** Bob sends  $t_B$  to Alice. Alice sends one bit to Bob: 1 if  $t_A = t_B$ , 0 otherwise. We distinguish now two cases:
- if  $t_A = t_B$ , Alice applies  $\mathcal{E}_{s_A}$  on registers  $A_kM_k\mathcal{G}_B$ , and sends back all her registers  $A_kM_kB_k = A_kM_k\mathcal{G}_B\mathcal{O}_B$  to Bob. This means that all registers are encrypted by  $s_A$  except  $\mathcal{O}_B$  which is encrypted only by Bob. Bob undoes the encryption for this qubit using the corresponding bits in  $s_B$  and outputs  $\mathcal{O}_B$ .
  - if  $t_A \neq t_B$ , Alice's state is totally mixed from Bob's randomness  $s_B$  and Bob has no quantum registers. Then, both players discard their quantum registers and start again from step 1, using fresh randomness for  $t_A, t_B, s_B$ .

**Remark 24.** Note that we can also start from a quantum protocol  $\Pi$ , first transform it into a memoryless quantum protocol  $\tilde{\Pi}$  as for instance in [11] and then define a private protocol  $\bar{\Pi}$  where the players encrypt and decrypt  $\tilde{\Pi}$ 's registers as described above. However, this would be at the expense of a quadratic blow-up in the communication cost while going from  $\Pi$  to  $\bar{\Pi}$ .

**Analysis of the protocol**

1. **Encrypted II:** For an odd round  $i$ , Alice sends registers  $A_i M_i B_i$  to Bob. We denote by  $T_A, T_B, S_B$  the registers corresponding to  $t_A, t_B, s_B$  respectively. The term appearing in CIC for this round is:

$$I(A_i M_i B_i : X | T_B S_B Y)_{\rho^{A_i M_i B_i X Y T_B S_B}} \leq I(A_i M_i B_i : X Y T_B S_B)_{\rho^{A_i M_i B_i X Y T_B S_B}} \quad (2)$$

where  $\rho^{A_i M_i B_i X Y T_B S_B}$  is of the form  $\mathbb{I}_{A_i M_i B_i} \otimes \rho^{X Y T_B S_B}$  (for some classical state  $\rho^{X Y T_B S_B}$ ), because of the quantum one time pad realized by Alice using her coins,  $T_A$ . Hence  $I(A_i M_i B_i : X | T_B S_B Y) = 0$ . We can prove a similar statement for even  $i$ .

2. **Encrypting and sending Bob's registers:** As above, this consists only of sending encryptions back and forth of quantum registers using fresh randomness. Similarly as in Equation 2, this does not give any information.
3. **Checking the coins:** When Bob sends  $t_B$  to Alice, her quantum state is totally encrypted by coins  $s_B$  (which are kept by Bob) hence her state is independent of  $t_B$ . Therefore, she does not receive any information about  $Y$  when she learns  $t_B$ . Then Alice checks whether  $t_A = t_B$  or not, and she sends the answer to Bob.
  - If  $t_A \neq t_B$ , then Bob knows only this information, which is independent of  $x$  so the term in CIC is zero. Then the players restart the process.
  - If  $t_A = t_B$ , Alice's quantum registers are fully encrypted by Bob which, as usual, does not contribute to CIC. After Alice's last message to Bob, let  $\rho_{final}$  the shared state. The contribution to CIC is

$$\begin{aligned} I(A_k M_k \mathcal{G}_B \mathcal{O}_B : X | T_B S_B Y)_{\rho_{final}} &= I(\mathcal{O}_B : X | T_B S_B Y)_{\rho_{final}} + I(A_k M_k \mathcal{G}_B : X | T_B S_B Y \mathcal{O}_B)_{\rho_{final}} \\ &\leq I(\mathcal{O}_B : X | T_B S_B Y)_{\rho_{final}} + I(A_k M_k \mathcal{G}_B : X T_B S_B Y \mathcal{O}_B)_{\rho_{final}} \\ &= I(\mathcal{O}_B : X | T_B S_B Y)_{\rho_{final}} \end{aligned}$$

where we used  $\rho_{final} = \rho_{final}^{A_k M_k \mathcal{G}_B} \otimes \rho_{final}^{X T_B S_B Y \mathcal{O}_B} = \mathbb{I}_{A_k M_k \mathcal{G}_B} \otimes \rho_{final}^{X T_B S_B Y \mathcal{O}_B}$  because of Alice's final encryption. We are in the case  $t_A = t_B$  so the output register is exactly the one of the original protocol, and therefore contributes  $I(\Pi_{out}(X, Y) : X | Y)$  to the total CIC.

The above analysis can be carried out at each repetition of these steps until the players have a run where they agree on their coins. Hence  $\bar{\Pi}$  has minimal CIC.

□

Our results imply that given any function  $f$ , if we take for  $\Pi$  the protocol where Alice just sends over  $x$  to Bob who computes and output  $f(x, y)$ , we obtain a protocol  $\Pi'$  that can perfectly compute  $f$  with CIC only the information gained from  $f(x, y)$ . Hence, we have the following Corollary.

**Corollary 3.** *For every input distribution  $\mu$ , and every positive integer  $k$ ,  $\text{CIC}_{\mu, k}^{\text{ML}, \text{C}}(f) = I(f(X, Y) : X | Y)$ , where  $(X, Y)$  is a random variable distributed according to  $\mu$ ,  $I$  denotes the (classical) conditional mutual information, and  $\text{CIC}_{\mu, k}^{\text{ML}, \text{C}}(f)$  denotes the minimum CIC achieved by a  $k$ -round memoryless quantum protocol with private classical coins to compute  $f$  exactly on input distribution  $\mu$ .*

Note that, in the case of AND, on distribution  $\mathcal{U}_0$  the output of  $\text{AND}(x, y) = x \wedge y$  is always 0. Hence, by the above result,  $\text{CIC}_{\mathcal{U}_0, k}^{\text{ML}, \text{C}}(\text{AND}) = \text{CIC}_{\mathcal{U}_0, k}^{\text{C}}(\text{AND}) = 0$  for every integer  $k$ .

## 5 One-shot coins

### 5.1 Definitions

In the previous section we saw that the model where quantum players have private coins allows for private protocols. While this implies that quantum communication can offer a new advantage compared to classical communication, it also shows that information complexity cannot provide non-trivial lower bounds for the quantum communication in this model. For this reason, we define a new model, where we restrict how the players can use these private coins. More precisely, we allow the players to use one-shot private coins, meaning that at each round they can only use fresh private coins which are independent of the previous and the future rounds.

**Definition 25.** Consider a quantum protocol with private coins. A coin is said to be one-shot if it is read only once or, in other words, if it is used only once by a unitary operation during any run of the protocol. The protocol is said to be one-shot coin if all its coins are one-shot.

One-shot coins are a very natural way of using coins. In the classical setting, every randomized protocol (without restriction on coins) can be simulated by a one-shot coin protocol with the same information and communication costs, since it is always possible to sample directly the messages [24].

More precisely, a memoryless quantum protocol  $\Pi$  with one-shot coins can be described as follows. At each round, a fresh set of coins is used. For odd (resp. even)  $i \in [k]$ , we denote by  $R_i^A$  (resp  $R_i^B$ ) the random variables corresponding to the coins used by Alice (resp. Bob) at round  $i$ . We note  $R^A = (R_i^A)_{i \in [k], i \text{ odd}}$  and  $R^B = (R_i^B)_{i \in [k], i \text{ even}}$ . For simplicity we use the same notation for the (classical) registers corresponding to these random variables. The interaction will be the following:

- The players start with classical respective registers  $X, R^A$  and  $Y, R^B$ . Alice starts with a quantum register  $M_0$ .
- At any odd round  $i$ , Alice applies an isometry from  $M_{i-1}$  to  $M_i$  using  $R_i^A$  as a classical control, and sends the whole quantum register  $M_i$  to Bob.
- At any even round  $i$ , Bob applies an isometry from  $M_{i-1}$  to  $M_i$  using  $R_i^B$  as a classical control, and sends the whole quantum register  $M_i$  to Alice.

Let us denote by  $\mathcal{T}_{\mu, \epsilon, k}^{\text{ML}, C_1}(f)$  the set of all  $k$ -round memoryless protocols  $\Pi$  with private one-shot coins computing function  $f$  with error at most  $\epsilon$  with respect to  $\mu$ .

**Definition 26.** The  $k$ -round  $\epsilon$ -error one-shot-coin memoryless classical input information complexity of  $f$  relative to distribution  $\mu$  is defined as  $\text{CIC}_{\mu, \epsilon, k}^{\text{ML}, C_1}(f) = \inf_{\Pi \in \mathcal{T}_{\mu, \epsilon, k}^{\text{ML}, C_1}(f)} \text{CIC}_{\mu}(\Pi)$ . We also define the quantity  $\text{CIC}_{\mu, \epsilon, k}^{C_1}(f)$  where we remove the memoryless constraint.

## 5.2 Relating $\text{CIC}_{\mathcal{U}_0, k}^{\text{ML}}$ and $\text{CIC}_{\mathcal{U}_0, k}^{\text{ML}, C_1}$ for the AND function

In this section, we show how to remove the one-shot coins from a memoryless quantum protocol with input distribution  $\mathcal{U}_0$  without increasing too much the information cost of the protocol.

**Theorem 4.** For every  $k$ -round memoryless quantum protocol  $\Pi$  with one-shot coins, we can construct a  $k$ -round memoryless protocol  $\Pi'$  without coins, which has the same behaviour distribution as  $\Pi$  and such that  $\text{CIC}_{\mathcal{U}_0}(\Pi') = O(\text{CIC}_{\mathcal{U}_0}(\Pi) \cdot (\log(k) + |\log \text{CIC}_{\mathcal{U}_0}(\Pi)|))$ .

Before proving this result (see Section 5.3 below), let us stress that for protocols computing (exactly) AND under distribution  $\mathcal{U}_0$ , this implies immediately

$$\text{CIC}_{\mathcal{U}_0, \epsilon, k}^{\text{ML}}(\text{AND}) = O\left(\text{CIC}_{\mathcal{U}_0, \epsilon, k}^{\text{ML}, C_1}(\text{AND}) \cdot \left(\log(k) + \left|\log \text{CIC}_{\mathcal{U}_0, \epsilon, k}^{\text{ML}, C_1}(\text{AND})\right|\right)\right).$$

Combining the above with Theorem 1, we obtain

**Corollary 27.** For every positive integer  $k$  and  $\epsilon > 0$ ,  $\text{CIC}_{\mathcal{U}_0, \epsilon, k}^{\text{ML}, C_1}(\text{AND}) = \Theta_{\epsilon}\left(\frac{1}{k}\right)$ .

This also implies that one-shot coins are very different than private coins in the quantum setting, since for the AND function, private coins allow for a private protocol, while one-shot coins do not.

## 5.3 Proof of Theorem 4

As we said, we will transform a memoryless quantum protocol  $\Pi$  with one-shot coins into a memoryless quantum protocol  $\Pi'$  without any coins, such that  $\Pi'$  will have the same outputs than  $\Pi$  and without increasing the information cost too much. The transformation from  $\Pi$  to  $\Pi'$  will informally be the following:

1. Quantize the coins from  $\Pi$  i.e., put them in quantum superposition in quantum registers  $\tilde{R}^A$  and  $\tilde{R}^B$ .
2. At each odd (or even) round, Alice (or Bob) applies the same transformation as in  $\Pi$ . Then, Alice (or Bob) would like to send all their quantum registers, including the coin registers, to the other player. Before doing that, Alice (or Bob) applies a compensation unitary that will limit the information cost increase that occurs because of the sending of all the quantum registers.

Step 1 is pretty straightforward. Step 2 will require a way to perform this compensation unitary, which will result in an increase in the information proportional to the binary entropy  $h_2$  at each round. While  $h_2$  is not convex, we show an weak-convexity result which will allow us to limit the total increase for all the rounds. The next subsection will deal with those two preliminary results.

### 5.3.1 Two useful lemmata

**Lemma 28.** *Consider a state  $\rho = \frac{1}{2} \sum_{x \in \{0,1\}} |x\rangle\langle x|_X \otimes |\phi_x\rangle\langle\phi_x|_{AB}$  for some pure states  $|\phi_x\rangle$ ,  $x \in \{0,1\}$ . There exist two unitary operators  $U_0, U_1$  acting on  $A$  such that if we define*

$$\rho' = \frac{1}{2} \sum_{x \in \{0,1\}} |x\rangle\langle x|_X \otimes (U_x \otimes I_B) |\phi_x\rangle\langle\phi_x|_{AB} (U_x^\dagger \otimes I_B),$$

we have  $I(X : AB)_{\rho'} \leq h_2\left(\frac{I(X:B)_\rho}{2}\right)$ .

*Proof.* For each  $x$ , let  $\rho_x = \text{Tr}_A |\phi_x\rangle\langle\phi_x|$ . By Uhlmann's theorem, there exists a unitary  $V$  acting on  $A$  such that  $\langle\phi_0| V |\phi_1\rangle = F(\rho_0, \rho_1)$ . Let  $U_0 = I$  and  $U_1 = V$ . We have

$$I(X : AB)_{\rho'} = h_2\left(\frac{1 - |\langle\phi_0| V |\phi_1\rangle|}{2}\right) = h_2\left(\frac{1 - F(\rho_0, \rho_1)}{2}\right) \leq h_2\left(\frac{I(X : B)_\rho}{2}\right),$$

where the first equality is by Lemma 16, the second equality is by definition of  $V$ , and the inequality is by Lemma 14.  $\square$

**Lemma 29.** *Let  $x_1, \dots, x_n \in [0, 1]$  and let  $S = \sum_i x_i$ . We have*

$$\sum_{i=1}^n h_2(x_i) \leq O(S \log(n) + S |\log(S)|)$$

with the convention that  $0 \log(0) = 0$ .

*Proof.* If  $S = 0$ , then  $x_i = 0$  for all  $i$  hence the property is true. From now on, assume  $S \neq 0$ . Let  $U = \frac{2n}{S}$  and  $x \in [0, 1]$ . Since  $U \geq 2$ , we have

- if  $x \geq \frac{1}{2}$ , then  $h_2(x) \leq 1 \leq 2x$
- if  $x \in [\frac{1}{U}, \frac{1}{2}]$ , then  $h_2(x) \leq 2x |\log(x)| \leq 2x |\log(U)|$
- if  $x \in [0, \frac{1}{U}]$ , then  $h_2(x) \leq h_2(\frac{1}{U}) \leq 2 \frac{|\log(U)|}{U}$ .

Since  $U \geq 2$ , for all  $x \in [0, 1]$ , we have  $2x \leq 2x |\log(U)|$  hence

$$h_2(x) \leq \max \left\{ 2x |\log(U)|, 2 \frac{|\log(U)|}{U} \right\} \leq 2 |\log(U)| \left( x + \frac{1}{U} \right). \quad (3)$$

Using the above for each  $x_i$  and summing over  $i$ , we obtain

$$\sum_{i=1}^n h_2(x_i) \leq 2 |\log(U)| \left( S + \frac{n}{U} \right).$$

Plugging the value of  $U$  in the above expression yields

$$\sum_{i=1}^n h_2(x_i) \leq 3S \left| \log \left( \frac{2n}{S} \right) \right| \leq O(S \log(n) + S |\log(S)|).$$

$\square$

### 5.3.2 Constructing $\Pi'$ from $\Pi$

We now prove Theorem 4.

*Proof of Theorem 4.* Consider a memoryless quantum protocol  $\Pi$ , described as in Section 5.1. Recall that:

$$\text{CIC}_{\mathcal{U}_0}(\Pi) = \sum_{i \text{ odd}} I(X : M_i | Y = 0, R^B) + \sum_{i \text{ even}} I(Y : M_i | X = 0, R^A).$$

Because the coins are independent of the inputs, we have

$$\text{CIC}_{\mathcal{U}_0}(\Pi) = \sum_{i \text{ odd}} I(X : M_i R^B | Y = 0) + \sum_{i \text{ even}} I(Y : M_i R^A | X = 0) \quad (4)$$

$$\geq \sum_{i \text{ odd}} I(X : M_i | Y = 0) + \sum_{i \text{ even}} I(Y : M_i | X = 0). \quad (5)$$

**Construction of  $\Pi'$ .** We start by quantizing the coins of  $\Pi$  using two quantum registers  $\tilde{R}^A$  and  $\tilde{R}^B$ .

- At the beginning of the protocol, Alice starts with registers  $\tilde{R}^A \otimes M_0 \otimes \tilde{R}^B$ .
- At each odd round  $i$ , Alice performs, as in  $\Pi$ , the isometry  $U_i$  on  $\tilde{R}_i^A M_{i-1}$  to obtain  $\tilde{R}_i^A M_i$ . This isometry uses the coin register only as a control string. Let  $\rho_i$  be the state of registers  $XY \tilde{R}_{\leq i}^A \tilde{R}_{\leq i}^B M_i \tilde{R}_{> i}^A \tilde{R}_{> i}^B$ . Alice holds all of them except  $Y$ . The registers  $\tilde{R}_{> i}^A \tilde{R}_{> i}^B$  have not been used yet by any player and contain a pure state independent of the players' other registers. Therefore,  $I(X : \tilde{R}_{> i}^A \tilde{R}_{> i}^B | Y = 0) = 0$  and  $I(X : M_i \tilde{R}_{> i}^A \tilde{R}_{> i}^B | Y = 0)_{\rho_i} = I(X : M_i | Y = 0)_{\rho_i}$ . Hence, we can apply Lemma 28, and obtain the existence of a unitary operation  $V_i^x$  on  $\tilde{R}_{\leq i}^A \tilde{R}_{\leq i}^B$  such that the resulting state  $\rho'_i = (I_{XY} \otimes V_i^x \otimes I_{M_i \tilde{R}_{> i}^A \tilde{R}_{> i}^B}) \rho_i (I_{XY} \otimes V_i^x \otimes I_{M_i \tilde{R}_{> i}^A \tilde{R}_{> i}^B})^\dagger$  satisfies

$$I(X : \tilde{R}_{\leq i}^A \tilde{R}_{\leq i}^B M_i \tilde{R}_{> i}^A \tilde{R}_{> i}^B | Y = 0)_{\rho'_i} \leq h_2 \left( \frac{I(X : M_i \tilde{R}_{> i}^A \tilde{R}_{> i}^B | Y = 0)_{\rho_i}}{2} \right) = h_2 \left( \frac{I(X : M_i | Y = 0)_{\rho_i}}{2} \right).$$

- At each even round  $i$ , we do exactly the same thing from Bob's side. The resulting state  $\rho'_i$  of  $\Pi'$  after step  $i$  satisfies

$$I(Y : \tilde{R}_{\leq i}^A \tilde{R}_{\leq i}^B M_i \tilde{R}_{> i}^A \tilde{R}_{> i}^B | X = 0)_{\rho'_i} \leq h_2 \left( \frac{I(Y : M_i \tilde{R}_{> i}^A \tilde{R}_{> i}^B | X = 0)_{\rho_i}}{2} \right) = h_2 \left( \frac{I(Y : M_i | X = 0)_{\rho_i}}{2} \right).$$

- Protocol  $\Pi'$  acts on the message registers similarly as in  $\Pi$  and Bob outputs therefore the same as in  $\Pi$ .

Let us now calculate the CIC of our new protocol  $\Pi'$ . Let  $k$  the number of rounds of  $\Pi$  (and hence  $\Pi'$ ).

$$\begin{aligned} \text{CIC}_{\mathcal{U}_0}(\Pi') &= \sum_{i \text{ odd}} I(X : \tilde{R}_{\leq i}^A \tilde{R}_{\leq i}^B M_i \tilde{R}_{> i}^A \tilde{R}_{> i}^B | Y = 0)_{\rho'_i} + \sum_{i \text{ even}} I(Y : \tilde{R}_{\leq i}^A \tilde{R}_{\leq i}^B M_i \tilde{R}_{> i}^A \tilde{R}_{> i}^B | X = 0)_{\rho'_i} \\ &\leq \sum_{i \text{ odd}} h_2 \left( \frac{I(X : M_i | Y = 0)_{\rho_i}}{2} \right) + \sum_{i \text{ even}} h_2 \left( \frac{I(Y : M_i | X = 0)_{\rho_i}}{2} \right) \end{aligned}$$

Let  $x_i = I(X : M_i | Y = 0)_{\rho_i}$  for  $i$  odd and  $x_i = I(Y : M_i | X = 0)_{\rho_i}$  for  $i$  even. Notice that  $\rho_i$  coincides with the state in  $\Pi$  on registers  $X, M_i, Y$  so those terms are exactly those of Equation 4, which gives  $S := \sum_i x_i \leq \text{CIC}_{\mathcal{U}_0}(\Pi)$ . Using Lemma 29, we can conclude that

$$\text{CIC}_{\mathcal{U}_0}(\Pi') \leq O(S \log(k) + S |\log(S)|) \leq O \left( \text{CIC}_{\mathcal{U}_0}(\Pi) \cdot \left( \log(k) + |\log \text{CIC}_{\mathcal{U}_0}(\Pi)| \right) \right).$$

□



**Acknowledgements** The authors would like to thank Rahul Jain, Virginie Leray, Ashwin Nayak and Dave Touchette for fruitful discussions. I. K. was supported by the ERC project QCC.

## References

- [1] Scott Aaronson and Andris Ambainis. Quantum search of spatial regions. *Theory Comput.*, 1:47–79, 2005.
- [2] Ziv Bar-Yossef, Thathachar S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. *SIAM J. Comput.*, 38(1):366–384, 2008.
- [3] Ziv Bar-Yossef, Thathachar S. Jayram, Ravi Kumar, and D. Sivakumar. An information statistics approach to data stream and communication complexity. *J. Comput. System Sci.*, 68(4):702–732, 2004.
- [4] Mark Braverman. Interactive information complexity. *SIAM J. Comput.*, 44(6):1698–1739, 2015.
- [5] Mark Braverman, Ankit Garg, Young Kun Ko, Jieming Mao, and Dave Touchette. Near-optimal bounds on bounded-round quantum communication complexity of disjointness. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science—FOCS 2015*, pages 773–791, 2015.
- [6] Mark Braverman, Ankit Garg, Denis Pankratov, and Omri Weinstein. From information to exact communication (extended abstract). In *STOC’13—Proceedings of the 2013 ACM Symposium on Theory of Computing*, pages 151–160, 2013.
- [7] Mark Braverman and Anup Rao. Information equals amortized communication. In *52nd Annual Symposium on Foundations of Computer Science—FOCS 2011*, pages 748–757, 2011.
- [8] Mark Braverman and Omri Weinstein. An interactive information odometer and applications. In *STOC’15—Proceedings of the 2015 ACM Symposium on Theory of Computing*, pages 341–350, 2015.
- [9] Harry Buhrman, Richard Cleve, John Watrous, and Ronald De Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.
- [10] Harry Buhrman, Richard Cleve, and Avi Wigderson. Quantum vs classical communication and computation. In *Proceedings of the 30th Annual Symposium on Foundations of Computer Science*, FOCS ’98, pages 63–68, 1998.
- [11] Harry Buhrman, Łukasz Czekaj, Andrzej Grudka, Michał Horodecki, Paweł Horodecki, Marcin Markiewicz, Florian Speelman, and Sergii Strelchuk. Quantum communication complexity advantage implies violation of a Bell inequality. *Proceedings of the National Academy of Sciences*, 113(12):3191–3196, 2016.
- [12] Amit Chakrabarti, Yaoyun Shi, Anthony Wirth, and Andrew Yao. Informational complexity and the direct sum problem for simultaneous message complexity. In *Proceedings of the 42nd IEEE symposium on Foundations of Computer Science*, FOCS ’01, pages 270–, 2001.
- [13] Omar Fawzi and Renato Renner. Quantum conditional mutual information and approximate Markov chains. *Comm. Math. Phys.*, 340(2):575–611, 2015.
- [14] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inform. Theory*, 45(4):1216–1227, 1999.
- [15] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separation for one-way quantum communication complexity, with applications to cryptography. *SIAM J. Comput.*, 38(5):1695–1708, 2008/09.
- [16] Jian-Yu Guan, Feihu Xu, Hua-Lei Yin, Yuan Li, Wei-Jun Zhang, Si-Jing Chen, Xiao-Yan Yang, Li Li, Li-Xing You, Teng-Yun Chen, Zhen Wang, Qiang Zhang, and Jian-Wei Pan. Observation of quantum fingerprinting beating the classical limit. *Phys. Rev. Lett.*, 116:240502, Jun 2016.
- [17] Rahul Jain and Ashwin Nayak. The space complexity of recognizing well-parenthesized expressions in the streaming model: the index function revisited. *IEEE Transactions on Information Theory*, 66(10):1–23, 2014.

- [18] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A lower bound for the bounded round quantum communication complexity of set disjointness. In *Proceedings of the 44th IEEE symposium on Foundations of Computer Science*, STOC '03, pages 220–229, 2003.
- [19] Iordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jeremie Roland, and David Xiao. Lower bounds on information complexity via zero-communication protocols and applications. In *Proceedings of the 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, FOCS '12, pages 500–509, 2012.
- [20] Iordanis Kerenidis, Mathieu Laurière, François Le Gall, and Mathys Rennela. Information cost of quantum communication protocols. *Quantum Inf. Comput.*, 16(3-4):181–196, 2016.
- [21] Bo'az Klartag and Oded Regev. Quantum one-way communication can be exponentially stronger than classical communication. In *Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing*, STOC '11, pages 31–40, 2011.
- [22] Eyal Kushilevitz and Noam Nisan. *Communication complexity*. Cambridge University Press, Cambridge, 1997.
- [23] Sophie Laplante, Mathieu Laurière, Alexandre Nolin, Jérémie Roland, and Gabriel Senno. Robust bell inequalities from communication complexity. In *11th Conference on the Theory of Quantum Computation, Communication and Cryptography*, 2016.
- [24] Mathieu Laurière and Dave Touchette. The flow of information in interactive quantum protocols: the cost of forgetting. *To appear in Innovations in Theoretical Computer Science (ITCS)*, 2017.
- [25] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.
- [26] Ran Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 358–367. ACM, 1999.
- [27] Dave Touchette. Quantum information complexity. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, pages 317–326. ACM, 2015.
- [28] Feihu Xu, Juan Miguel Arrazola, Kejin Wei, Wenyan Wang, Pablo Palacios-Avila, Chen Feng, Shihan Sajeed, Norbert Lutkenhaus, and Hoi-Kwong Lo. Experimental quantum fingerprinting with weak coherent pulses. *Nature communications*, 6, October 2015.